SOLE SOURCE JUSTIFICATION FORM

For Internal Use Only

Contact Name: *Manos Antonakakis* **Date:** *12/9/2016*

Provide contact information. Check the box next to your preferred method of communication.

☐ Phone

☑ Email *manos@gatech.edu*

Requisition # *82258487*

Proposed Source:

Supplier Name: *Neustar*

Contact Name: *Rodney Joffe*

Telephone: *6024186471* **Fax:**

Email: *Rodney.Joffe@neustar.biz*

What is the purpose of this purchase? Click here for instructions

We need the Neustar data to model network activities that attacks conduct in the cyber domains so we can perform against the DARPA project with number 2106DTX. What we need is: Network pcaps for: TLD/gTLD traffic, ANS DNS traffic, UltraDNS Recursive traffic, Web Proxy/WebRedirect HTTP Traffic, DDoS Mitigation traffic, SLD traffic.

☐ Environmental Health and Safety **IS REQUIRED** and ATTACHED. Click here for information

☑ Environmental Health and Safety **IS NOT REQUIRED.**

If the requested product is an integral part or accessory compatible with existing equipment please provide the following information:

Existing equipment:

Manufacturer:

Model/Serial #: **GT #** **Dollar Value:**

Why is this the only available source/supplier? Click here for instructions

In the last 10 years I invented the security DNS analysis and mining fields. As an expert I can categorically say that nobody else in the world can give the visibility and granularity necessarily for the completion of the DARPA project with number 2106DTX. Again, nobody else in the world can provide these datasets and the granularity we want for the DARPA project. Neustar run the TLD, gTLD and ANS servers for a large number of zones in the global Internet. At the same time the run a worldwide open recursive platform for which they maintain pcap level DNS traffic going back several years. These datasets cannot be found anywhere else in the world, simply because Neustar is the only company that runs the infrastructure for these TLDs, gTLDs, ANSs, and RDNS servers. Thus, being the owner of these servers makes them the only source that can provide data like these.

SOLE SOURCE JUSTIFICATION FORM

For Internal Use Only

Are there any extenuating circumstances or considerations?

Not to my knowledge.

Is there a requirement for a sole brand? Click here for instructions

Not to my knowledge.

What efforts have you made to find other sources? Click here for instructions

I am a member and co-chair of MAAWG (https://www.m3aawg.org/) over the last 5 years, where all magor telecommunication companies come to meet. If an other vendor like Neustar existed that could offer these data it would be there. No other vendor can provide this visibility to us.

Provide a price quote or price analysis for this request. Click here for instructions

Attach a quote from supplier for similar goods/services or Cost Analysis. Purchasing will review documents for price reasonableness.

Sinness, Mark B

From:	Manos Antonakakis <antonakakis@gmail.com>
Sent:	Thursday, December 22, 2016 2:58 PM
To:	Sinness, Mark B
Subject:	Re: Items needed to complete POs

Hey Mark,

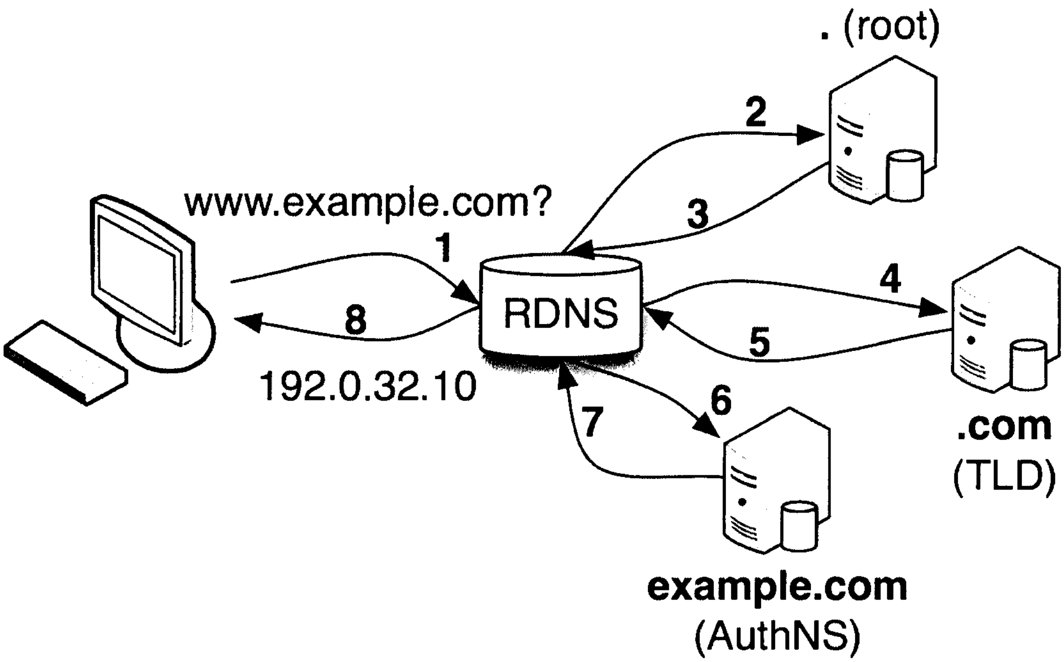
Let me try to explain why Neustar and KDT are single source providers.

Lets begin by explaining briefly how the Domain Name System (DNS) works. DNS is a distributed hierarchical database that maps domain names (i.e., example.com or google.com) to IP addresses.

When your laptop makes a DNS resolution request for "example.com", you will be contacting a recursive DNS server (RDNS). This is the step 1 in the in line figure. If the RDNS does not have the mapping between "example.com" to its IP address, it will have to contact in series:

1. The root servers (steps 2 & 3)
2. The Top Level Domain (TLD) names servers (steps 4 & 5), and finally
3. The Authoritative DNS (AuthNS) servers (steps 6 & 7).

At that point the AuthNS server will provide back a valid mapping between "example.com" and an IP address. Then, the RDNS will yield back this answer to your laptop (step 8) and the DNS communication will end.



Now, Neustar and KDT are single source providers because they are the organizations that operate, own and have physical control over the these TLD and AuthNS servers. As you can imagine, there is only one entity in the world that is responsible for a TLD or an ANS server. For, Neustar is responsible for 4 TLDs, 24 gTLD and 32 open RDNS servers world wide. This means that *only Neustar* can see the traffic that comes and leaves from these servers *at world-wide scale and in a complete sense (that is not partial DNS visibility)*. In a similar sense, KDT runs a number of very large AuthNS servers too, which makes them single source providers for the data we need from these AuthNS servers.

Thus, as you can imagine, these DNS traffic datasets I need for my project, cannot be seen, captured, and effectively purchased by anyone else than Neustar and KDT. Therefore, Neustar and KDT are single source providers for our project.

Would this explanation suffice or you want me to break this down even further?

Thanks,

Manos